состояния в компьютерных сетях / А. А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84. ***7.*** *Параметры прогнозирования и идентификации атак в информационно-комуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. – 2014. – Том 16. – №1. – С. 89-95.* ***8.*** *Гізун А. І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В. В. Волянська, В. О. Риндюк, С. О. Гнатюк // Захист інформації. – 2013. – №1 (58). – С.66-75.* ***9.*** *Стасюк А. И. Базовая модель параметров для построения систем выявления атак / А. И. Стасюк, А. А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.* ***10.*** *Корченко А. А. Метод формирования лингвистических эталонов для систем выявления вторжений / А. А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.* ***11.*** *Гізун А. І. Формалізована модель побудови евристичних правил для виявлення інцидентів // А. І. Гізун, В. О. Гнатюк, О. М. Супрун / Вісник Інженерної академії України. – 2015. – №1. – С. 110-115.* ***12.*** *Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями // А. О. Корченко, В. А. Козачок, А. І. Гізун // Захист інформації. – 2015.– Т.17. – №1. – С. 86-98.* ***13.*** *Корченко А. О. Кортежная модель формирования набора базовых компонент для выявления кибератак / А. А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.*

Сергій Гончар, Геннадій Леоненко, Олексій Юдін
ДержНДІ Спецзв'язку

УДК 004.056.5

ЗАГАЛЬНА МОДЕЛЬ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ АСУ ТП

Анотація: **Запропонована загальна модель загроз безпеці інформації в автоматизованих системах управління технологічними процесами об'єктів критичної інфраструктури, яка враховує технічний та соціокультурний компоненти системи захисту інформації.**
Summary: **Offered general model of information security threats in industrial control systems of critical information objects, which takes into account technical and sociocultural components of information protection system.**
Ключові слова: **АСУ ТП, критична інфраструктура, захист інформації, соціокультурний компонент, модель загроз.**

І Вступ

Сьогодні практично всі держави світу залежать від автоматизації виробничих процесів, а саме, від безперебійної роботи автоматизованих систем управління технологічними процесами (АСУ ТП). Найбільш значущими АСУ ТП є ті, що забезпечують роботу об'єктів критичної інфраструктури (ОКІ). Під ОКІ будемо розуміти атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства тощо [1]. Таким чином, від ступеню захищеності АСУ ТП ОКІ залежить не тільки прибуток крупних компаній (корпорацій), але й національна або регіональна безпека [2]. Викладене вище робить актуальною задачею розробку та впровадження систем захисту ОКІ, в тому числі і АСУ ТП. Термін «система захисту інформації ОКІ» визначимо як взаємопов'язану сукупність організаційних, нормативно-правових, науково-методичних та технічних заходів, засобів і методів захисту інформації, спрямованих на унеможливлення витоку, знищення, блокування, порушення цілісності та режиму доступу до інформації [3].

У класичній інфраструктурі інформаційних технологій вже давно існує множина способів і методів забезпечення захисту інформації. Натомість організаційно-технічні рішення щодо захисту АСУ ТП ОКІ повинні бути суттєво змінені з урахуванням специфіки виробничих процесів підприємств. Внаслідок цього, для ряду завдань, наприклад, таких, які потребують прийняття рішення у режимі реального часу, часто необхідно не просто доопрацювання засобів захисту, а їх розробка з нуля з урахуванням додаткових вимог.

З урахуванням викладеного здійснимо декомпозицію системи захисту АСУ ТП ОКІ на складові частини. Так, на нашу думку, система захисту складається з:

- нормативно-правової бази;
- науково-методичної бази;
- організаційно-технічних і режимних заходів;
- персоналу забезпечення.

При цьому персонал забезпечення, який виділений в окрему складову системи захисту, може бути і джерелом загроз [4]. Так, результати аналізу джерел порушень безпеки в інформаційних системах [5] свідчать, що близько 70 відсотків порушень відбуваються через персонал забезпечення, рис. 1.

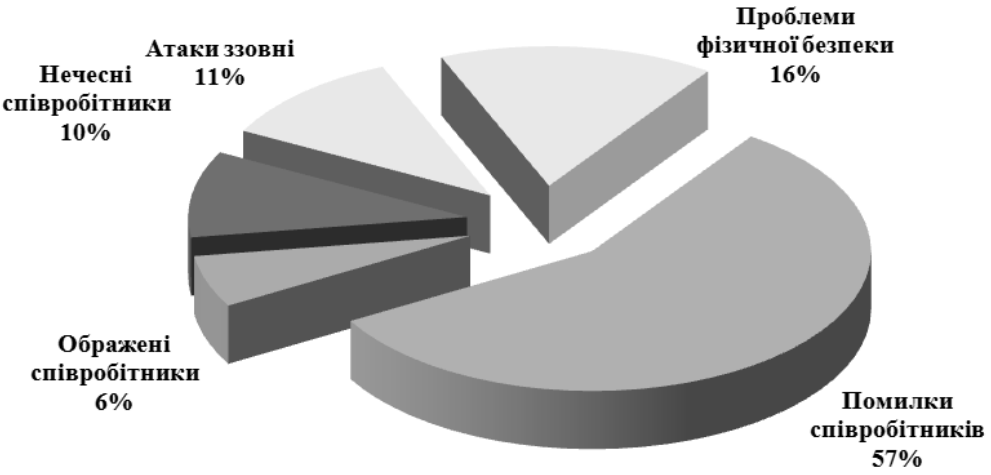

Рисунок 1 - Джерела порушень безпеки

У той же час аналіз реальних інцидентів в АСУ ТП (рис. 2) показує, що доля порушень, яка припадає на персонал забезпечення, менша ніж в інших автоматизованих системах [6].

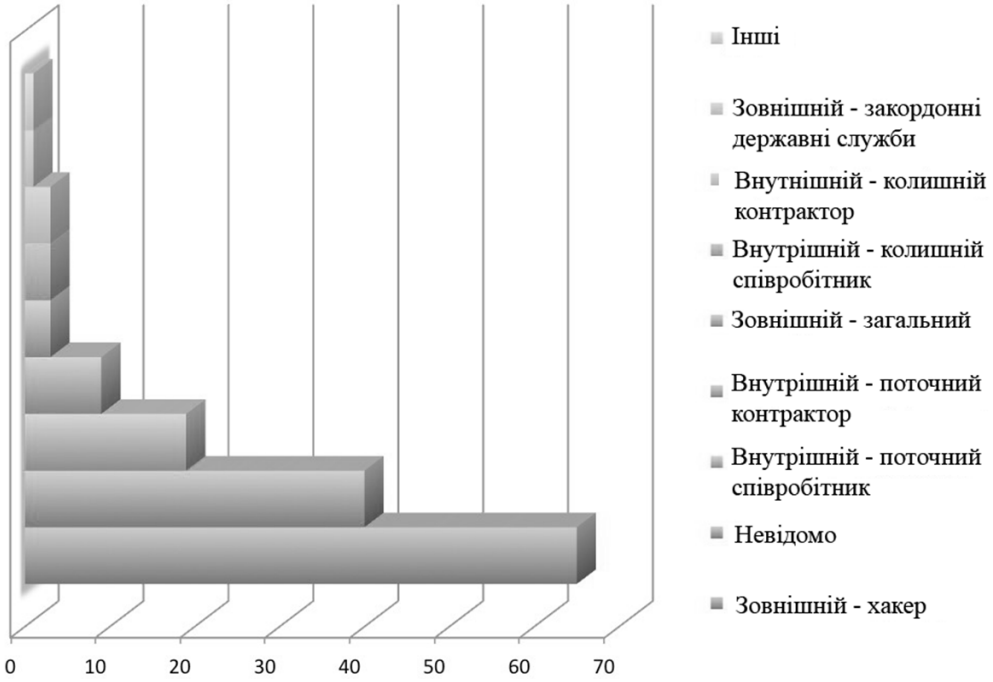

Рисунок 2 - Тип порушника АСУ ТП

Загрози з боку персоналу забезпечення, як правило, реалізуються завдяки інформаційно-психологічному впливу, незадоволеності потреб особистості, міжособистісного вербального обміну персоналу забезпечення тощо. Таким чином, можна стверджувати, що один з аспектів досягнення інформаційної безпеки розкривається через забезпечення захищеності інтелектуальної, психологічної, культурної, світоглядної та інших видів людських потреб, тобто – соціокультурний аспект. Соціокультурний аспект інформаційної безпеки як основний об’єкт захисту передбачає особистість (персонал забезпечення) і, в першу чергу, спрямований на захищеність потреб особистості в інформації, яка необхідна для забезпечення життєдіяльності, освіти, функціонування тощо [7].

Різний рівень соціально-економічних, соціокультурних та інших відносин буде спричиняти і різний рівень інформаційної безпеки. У той же час соціально-економічні, соціокультурні та інші відносини, в свою чергу, залежать від рівня обізнаності суб’єктів політико-економічного життя, які визначають одночасно і ступінь адекватності сприйняття ними навколишньої дійсності, і, як наслідок, обґрунтування прийнятих рішень і дій. Отже, саме рівень соціально-економічних, соціокультурних та інших відносин може формувати

відповідний рівень інформаційної безпеки, і саме соціокультурний аспект буде мати значний вплив на інформаційну безпеку ОКІ.

Зважаючи на викладене вище, зробимо висновок, що загальна структура системи захисту інформації АСУ ТП ОКІ буде складатися із найбільш значущих компонентів - технічного та соціокультурного. Складові системи захисту інформації АСУ ТП ОКІ, такі як нормативно-правова та науково-методична бази, виключимо з загальної структури, тому що вони не суттєво піддаються зовнішнім дестабілізуючим впливам.

ІІ Загальна модель загроз захисту інформації АСУ ТП

З урахуванням обмежень, викладених вище, пропонуємо до розгляду загальну модель загроз захисту інформації окремої АСУ ТП, рис. 3.

Під зовнішнім дестабілізуючим впливом маємо на увазі сукупність певних множин загроз:

- $v = \overline{1,V}$ - множина загроз несанкціонованого доступу до інформації, несанкціонованих змін або викрадення інформації, відмова в обслуговуванні або профілактика авторизованого доступу, відмова від дії, яка мала місце, або вимога підтвердження дії, якої не було;

- $s = \overline{1,S}$ - множина загроз реалізації інформаційно-психологічного впливу на персонал забезпечення АСУ ТП.

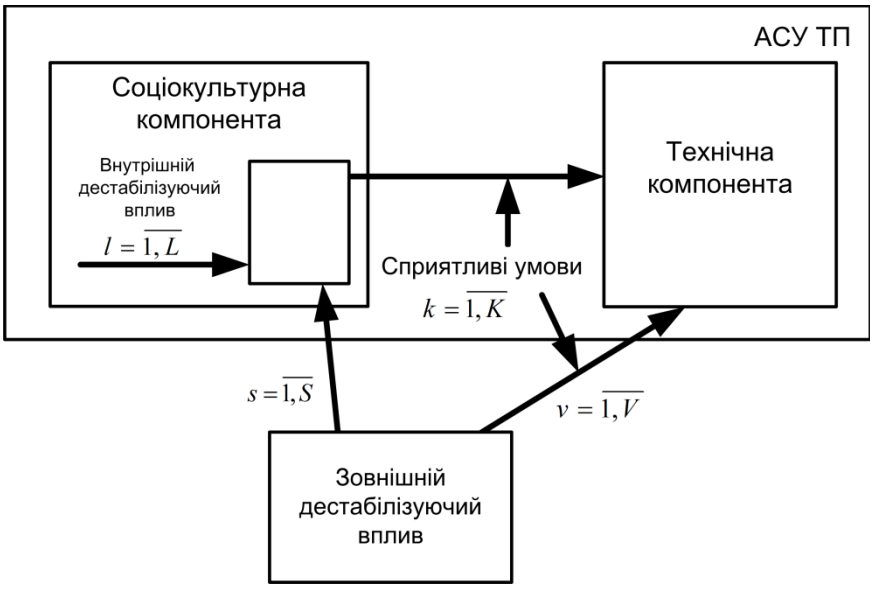

Рисунок 3 - Загальна модель загроз захисту інформації АСУ ТП

Множина факторів внутрішнього дестабілізуючого впливу $l = \overline{1,L}$, що являє собою множину людських потреб, через захищеність яких може розкриватися забезпечення інформаційної безпеки АСУ ТП [8]:

- вітальні (природні): їжа, одежа, житло, відпочинок, комфорт, екологія тощо;
- самоактуалізація (пізнавальні): активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;
- інтелектуальні (наукові): освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;
- психічні (естетичні): прив'язаність, спорідненість, чиста совість, піднесеність тощо;
- соціальні (групові): спілкування, засоби спілкування, увага до себе, спільна діяльність тощо;
- самореалізація (індивідуальні): творчість, самовдосконалення, самоповага, повага зі сторони інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;
- духовні (етичні): щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

Таким чином, модель загроз АСУ ТП у загальному виді можна представити у вигляді формальної функціональної залежності:

$$z = F(v, s, l, k). \tag{1}$$

Очевидно, що забезпечення інформаційної безпеки окремої АСУ ТП може бути реалізовано лише в тому випадку, якщо буде забезпечена інформаційна безпека технічного компонента та інформаційна безпека соціокультурного компонента.

Крім того, загальна модель загроз захисту інформації окремої АСУ ТП, рис. 3, показує, що загрози для інформаційної безпеки АСУ ТП будуть визначатися як зовнішніми дестабілізуючими впливами: атаками на технічний компонент $v=\overline{1,V}$ і інформаційно-психологічними впливами на соціокультурний компонент $s=\overline{1,S}$, так і внутрішніми дестабілізуючими впливами: використання зловмисниками людських потреб персоналу забезпечення $l=\overline{1,L}$.

Разом з тим необхідно зазначити, що кінцевою метою зловмисників є реалізація загроз саме по відношенню до технічного компонента: порушення конфіденційності, цілісності, доступності та неспростовності інформації. Тобто, діючи на соціокультурний компонент, зовнішні та/або внутрішні дестабілізуючі впливи можуть побудити об'єкт їх впливу до деструктивних дій відносно технічного компонента.

Крім того, ймовірність реалізації загроз відносно технічного компонента, як з боку соціокультурного компонента (під дією внутрішніх та/або зовнішніх дестабілізуючих впливів), так і безпосередньо з боку зовнішніх дестабілізуючих впливів, буде залежати від наявності сприятливих для цього умов $k=\overline{1,K}$. Розглянемо даний аспект більш детально.

Нехай R_v – подія, яка відображає реалізацію загрози шляхом атаки на технічний компонент, R_s – подія, яка відображає реалізацію загрози щодо технічного компонента від інформаційно-психологічного впливу на соціокультурний компонент, R_l – подія, яка відображає реалізацію загрози щодо технічного компонента від незахищеності людських потреб персоналу забезпечення, а Q_k – подія, яка відображає наявність сприятливих умов із множини $k=\overline{1,K}$, для реалізації загроз. Для спрощення припустимо, що події R_v, R_s, R_l незалежні і складають повну групу несумісних подій.

Отже, ймовірність реалізації *v*-ї загрози від атаки на технічний компонент визначатиметься наступним чином:

$$P(R_v)=\sum_{k=1}^{K}P(R_v \mid Q_k)P(Q_k), \tag{2}$$

де ймовірність реалізації *s*-ї загрози щодо технічного компонента від інформаційно-психологічного впливу на соціокультурний компонент буде визначатися з виразу:

$$P(R_s)=\sum_{k=1}^{K}P(R_s \mid Q_k)P(Q_k), \tag{3}$$

а ймовірність реалізації *l*-ї загрози щодо технічного компонента від незахищеності людських потреб персоналу забезпечення можна представити у вигляді:

$$P(R_l)=\sum_{k=1}^{K}P(R_l \mid Q_k)P(Q_k), \tag{4}$$

де $P(R_v \mid Q_k)$ - ймовірність реалізації *v*-ї загрози за умови наявності сприятливих умов Q_k;

$P(R_s \mid Q_k)$ - ймовірність реалізації *s*-ї загрози за умови наявності сприятливих умов Q_k;

$P(R_l \mid Q_k)$ - ймовірність реалізації *l*-ї загрози за умови наявності сприятливих умов Q_k;

$P(Q_k)$ - ймовірність наявності сприятливих умов.

Таким чином, ймовірність реалізації загроз за умови наявності сприятливих умов можливо представити у вигляді матриці:

$$P\left(R_{v,s,l}\right)=\begin{bmatrix} P\left(R_v\right) \\ P\left(R_s\right) \\ P\left(R_l\right) \end{bmatrix}. \quad (5)$$

Елементи матриці (5) будуть визначатися з виразів (2), (3), (4).

Враховуючи припущення, що події R_v, R_s, R_l незалежні і несумісні, ймовірність реалізації загрози захисту інформації в АСУ ТП можна представити у вигляді:

$$P(R)=\sum_{v=1}^{V}P\left(R_v\right)+\sum_{s=1}^{S}P\left(R_s\right)+\sum_{l=1}^{L}P\left(R_l\right). \quad (6)$$

Очевидно, що захист інформації буде забезпечено у випадку, якщо:

$$P\left(R\right)=0. \quad (7)$$

III Висновки

Враховуючи викладене можна сформулювати наступні висновки:

- загрози і відповідно й механізми захисту АСУ ТП і звичайних автоматизованих систем відрізняються;
- значний вплив на інформаційну безпеку ОКІ має соціокультурний аспект;
- для розробки адекватних рекомендацій, методів та засобів щодо захисту інформації в АСУ ТП можливо застосовувати запропоновану загальну модель загроз захисту інформації АСУ ТП;
- при здійсненні розрахунку ймовірності реалізації загроз від атак на технічний компонент необхідно враховувати дію дестабілізуючих впливів на соціокультурний компонент.

Список використаної літератури: ***1.*** *Васильєв Ю. К. Аналіз міжнародного досвіду щодо визначення ключових систем інформаційної інфраструктури / Васильєв Ю. К. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – Вип. 1(27). – С. 43-47.* ***2.*** *Леоненко Г. П., Юдин А. Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. -2013. – Вип. 1(3). - С. 44.* ***3.*** *Гончар С. Ф. Методологічні засади розробки та впровадження систем захисту інформації на об'єктах критичної інфраструктури / Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. - Вип. 1(25). – С. 158-163.* ***4.*** *Гончар С. Ф. Анализ угроз и уязвимостей индустриальных автоматизированных систем управления / Гончар С. Ф., Леоненко Г. П., Юдин А. Ю. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Вип. 2(26). – С. 9-14.* ***5.*** *Анализ угроз сетевой безопасности [Електронний ресурс]. – Режим доступу: http://ypn.ru/138/analysis-of-threats-to-network-security/6/.* ***6.*** *Лукацкий Алексей. Статистика реальных инцидентов ИБ в индустриальных системах [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/blog/personal/Business_without_danger/38672.php.* ***7.*** *Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Соціокультурний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури : тези доповідей XX Всеукраїнської науково-практичної конференції «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення», Житомир, – 2014. - С. 195-196.* ***8.*** *Ловцов Д. А., Сергеев Н. А. Управление безопасностью эргасистем / Под ред.. Д. А. Ловцова, - 2-е изд. испр. и доп. – М.: РАУ-Университет, 2001. - 224 с.*

Елена Азаренко, Олег Бляшенко, Михаил Дивизинюк, Валерия Ковач
Государственное учреждение «Институт геохимии окружающей среды НАН Украины»

УДК 504.455.064.3:574 (262.5)

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Аннотация: **Показано, что системы мониторинга чрезвычайных ситуаций являются гибридными системами с аналого-цифровой обработкой передаваемой информации. Защита информации, циркулирующей в ней, должна основываться на наличии в ее составе трех типов подсистем, каждая из которых должна отвечать своим специфическим требованиям.**